Homework 4

Mark Schulist

1)

1.a)

$$\begin{aligned} &x \equiv 3 \bmod 10 \implies x \equiv 1 \bmod 2 \quad x \equiv 3 \bmod 5 \\ &x \equiv 11 \bmod 17 \implies x \equiv 2 \bmod 9 \quad x \equiv 1 \bmod 2 \\ &x \equiv 14 \bmod 27 \implies x \equiv 5 \bmod 9 \end{aligned} \tag{1}$$

Here we get incompatible equations, in particular the ones that claim $x \equiv 2 \bmod 9$ and $x \equiv 5 \bmod 9$. There is no solution to x where both of these can be satisfied.

1.b)

$$\begin{aligned} &x \equiv 5 \bmod 8 \implies x \equiv 1 \bmod 2 \\ &x \equiv 5 \bmod 12 \implies x \equiv 2 \bmod 3 \quad x \equiv 1 \bmod 4 \\ &x \equiv 11 \bmod 45 \implies x \equiv 1 \bmod 5 \quad x \equiv 2 \bmod 9 \end{aligned} \tag{2}$$

Combining we get:

$$\begin{cases} x \equiv 5 \bmod 8 \\ x \equiv 2 \bmod 9 \\ x \equiv 1 \bmod 5 \end{cases} \tag{3}$$

Our $m = 8 \cdot 5 \cdot 9 = 360$.

$$\begin{aligned} b_1 &= \left(\frac{360}{8}\right)^{-1} = 45^{-1} = 5^{-1} = 5 \bmod 8 \\ b_2 &= \left(\frac{360}{9}\right)^{-1} = 40^{-1} = 4^{-}1 = 7 \bmod 9 \\ b_3 &= \left(\frac{360}{5}\right)^{-1} = 72^{-1} = 2^{-1} = 3 \bmod 5 \end{aligned} \tag{4}$$

Hence $x = 45 \cdot 5 \cdot 5 + 40 \cdot 7 \cdot 2 + 72 \cdot 3 \cdot 1 = 101 \bmod 360$.

2)

2.a)

When is $\phi(n)$ even?

$$\phi(n) = \prod_{i=1}^{r} p_i^{a-1}(p_i - 1) \tag{5}$$

If $\phi(n)$ has a factor of 2, then it will be even, so we need to ensure that both (a) $p_i^a - 1$ AND (b) $p_i - 1$ are odd. The only even prime is 2, so we know that the only prime which can make (b) odd is 2. Additionally,

we know that (a) cannot be even, and the only way to make 2^k odd is if $k = 0 \implies a - 1 = 0 \implies a = 1$. Hence $n = 2$ is the only nontrivial solution.

If $n = 1$, it has no factors (other than 1) and $|(\mathbb{Z}/\mathbb{Z})^\times| = 1$ which is odd.

2.b)

When is $\phi(n) = \phi(2n)$?

We know that $\phi(2) = 1$.

If n is odd, then $(n, 2) = 1$. Hence $\phi(2n) = \phi(2)\phi(n)$ so $\phi(n) = \phi(2n)$.

If n is even, then $n = 2^k m$ where m is odd. Hence $\phi(2n) = \phi\big(2^{k+1}\big)\phi(m) \implies \phi(2n) \neq \phi(n)$.

So this fact is only true when n is odd.

2.c)

$\phi(n) = 14$ for what n?

We know that $14 = 2 \cdot 7$. Using Equation 5 we can see that because 14 only has 2 factors, we can only use one prime to satisfy $\phi(n) = 14$. We know that the second term must equal 2 because if the first term was 2, then the second would be 1 which is not 7. Hence $p_i - 1 = 2 \implies p_i = 3$. That means that we need to find a value for a such that $7 = 3^{a-1}$, but there is no solution in $\mathbb{Z}$. Hence there is no value of n where $\phi(n) = 14$.

3)

Proof.

Fix k to equal an $\phi(n)$.

We can first show that a particular inequality holds, and then use it show that n is bounded above. We want to show that $p - 1 > \sqrt{\frac{p}{4}} \forall p$ primes.

$$
\begin{aligned}
p &> 1 \\
p &> \frac{9 + \sqrt{17}}{8} \\
p &> \sqrt{\frac{17}{64}} + \frac{9}{8} \\
\left(p - \frac{9}{8}\right)^2 &> \frac{17}{64} \\
p^2 - \frac{9}{4}p + \frac{81}{64} &> \frac{17}{64} \\
p - \frac{9}{4}p + 1 &> 0 \\
p^2 - 2p + 1 &> \frac{p}{4} \\
p - 1 &> \sqrt{\frac{p}{4}}
\end{aligned}
\tag{6}
$$

On paper I started in the reverse direction to show the above inequality holds, which is why it looks a bit contrived in this form...

$$\begin{aligned} \phi(n) = \prod_{i=1}^{r} p_i^{a-1}(p_i - 1) \leq \prod_{i=1}^{r}(p_i - 1) < \sqrt{\frac{n}{4}} \\ \phi(n) > \sqrt{\frac{n}{4}} \\ k > \sqrt{\frac{n}{4}} \\ 4k^2 > n \end{aligned} \tag{7}$$

Since n is bounded above, $\phi(n) = k$ has finitely many solutions. Looking back, this is a pretty loose bound but at least it's finite! □

4)

4.a)

$$x^3 + 2x - 3 = 0 \bmod 45 \tag{8}$$

For mod 9, the solutions are $x = 1, 2, 6$ (by brute force on mod 9).

For mod 5, the solutions are $x = 1, 3$.

So we know there are 6 total solutions.

$$\begin{aligned} b_1 = 5^{-1} = 2 \bmod 9 \\ b_2 = 9^{-1} = 4 \bmod 5 \end{aligned} \tag{9}$$

For $(1, 1)$: $x = 2 \cdot 5 \cdot 1 + 4 \cdot 9 \cdot 1 = 46 = 1 \bmod 45$.
For $(1, 3)$: $x = 2 \cdot 5 \cdot 1 + 4 \cdot 9 \cdot 3 = 118 = 28 \bmod 45$.
For $(2, 1)$: $x = 2 \cdot 5 \cdot 2 + 4 \cdot 9 \cdot 1 = 56 = 11 \bmod 45$.
For $(2, 3)$: $x = 2 \cdot 5 \cdot 2 + 4 \cdot 9 \cdot 3 = 128 = 38 \bmod 45$.
For $(6, 1)$: $x = 2 \cdot 5 \cdot 6 + 4 \cdot 9 \cdot 1 = 96 = 6 \bmod 45$.
For $(6, 3)$: $x = 2 \cdot 5 \cdot 6 + 4 \cdot 9 \cdot 3 = 168 = 33 \bmod 45$

4.b)

$$x^2 + 5x - 13 = 0 \bmod 154 \tag{10}$$

$$154 = 11 \cdot 7 \cdot 2 \tag{11}$$

If we look at $x^2 + 5x - 13 = x^2 + x + 1 = 0 \bmod 2$, we can see that it has no solutions for x. Therefore, the overall polynomial cannot have any solutions.

5)

We want to determine the number of solutions if n is square-free and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $x^2 = a \bmod n$ has at least one solution.

If n is square-free, then $n = \prod_{i=1}^{k} p_i$ (the exponent on each prime is either 0 or 1 and n has k prime factors).

We know that $x^2 = a \bmod p$ for odd primes ($p \neq 2$) p has exactly 2 solutions.

$$x^2 = a \bmod n \implies \begin{cases} x^2 = a \bmod p_2 \Rightarrow 2 \text{ sol} \\ x^2 = a \bmod p_2 \Rightarrow 2 \text{ sol} \\ \dots \\ x^2 = a \bmod p_k \Rightarrow 2 \text{ sol} \end{cases} \tag{12}$$

So if n is odd, then there are 2^k solutions.

And if n is even, then there are 2^{k-1} solutions (as one of the factors is $p = 2$ which only has one solution).

6)

6.a)

if $f(x) = 0 \bmod p$ then $x = \frac{-b \pm \sqrt{\Delta}}{2a} \bmod p$, which has 2 unique solutions if $\sqrt{\Delta} \neq -\sqrt{\Delta}$. $\sqrt{\Delta} \neq -\sqrt{\Delta}$ if and only if $\Delta \neq 0$. In other words, if $\Delta = 0$ then x has 1 solution and if $\Delta \neq 0$ then x has 2 solutions.

Notice that the same also holds for $x^2 = \Delta \bmod p$. $x^2 = \Delta \bmod p$ has 2 solutions if $\Delta \neq 0$ and 1 solution if $\Delta = 0$. Hence quadratic polynomials have at most 2 roots mod prime p.

6.b)

6.b.a)

$$x^2 + 5x - 15 = 0 \bmod 17 \tag{13}$$

$$\begin{aligned} x &= \frac{-5 \pm \sqrt{25 + 60}}{2} \\ &= \frac{-5 \pm \sqrt{85}}{2} \\ &= \frac{-5 \pm \sqrt{0}}{2} \\ &= \frac{12}{2} \\ &= 6 \end{aligned} \tag{14}$$

6.b.b)

$$x^2 + 3x - 8 = 0 \bmod 37 \tag{15}$$

$$
\begin{aligned}
x &= \frac{-3 \pm \sqrt{9+32}}{2} \\
&= \frac{-3 \pm \sqrt{41}}{2} \\
&= \frac{-3 \pm 2}{2} \\
&= \frac{34 \pm 2}{2} \\
\implies \quad x &= 16, 18
\end{aligned}
\tag{16}
$$

6.c)

We want to show the zeros of all 4 quadratic polynomials in $\mathbb{Z}/2\mathbb{Z}$.

$$
\begin{aligned}
x^2 + x + 1 = 0 &\implies \emptyset \\
x^2 + 1 = 0 &\implies \{1\} \\
x^2 = 0 &\implies \{0\} \\
x^2 + x = 0 &\implies \{0, 1\}
\end{aligned}
\tag{17}
$$

7)

7.a)

$$
x^2 + 11x - 5 = 0 \bmod 71 \tag{18}
$$

$$
\frac{-11 \pm \sqrt{11^2 + 20}}{2} = \frac{-11 \pm \sqrt{70}}{2} \tag{19}
$$

But $y^2 = 70$ does not have any solutions in mod 71. So x has no solutions mod 71.

7.b)

$$
4x^2 + 2x + 5 = 0 \bmod 55 \tag{20}
$$

$$
\begin{aligned}
4x^2 + 2x + 5 &= 0 \bmod 5 \\
x^2 &= \Delta \bmod 5 \\
x^2 &= 4 \bmod 5
\end{aligned}
\tag{21}
$$

So this part “brings” 2 solutions.

$$
\begin{aligned}
4x^2 + 2x + 5 &= 0 \bmod 11 \\
x^2 &= \Delta \bmod 11 \\
x^1 &= 1 \bmod 11
\end{aligned}
\tag{22}
$$

And this part also brings 2 solutions.

So $2 \cdot 2 = 4$ so there are 4 possible solutions.

7.c)

$$
x^2 - 5x + 16 = 0 \bmod 30 \tag{23}
$$

$$\begin{aligned}\Delta = 25 - 64 = -39 &= 1 \bmod 2 \\ &= 0 \bmod 3 \\ &= 1 \bmod 5\end{aligned} \tag{24}$$

When $\Delta = 0 \bmod 3$, we know that this will give us 1 solution due to problem (6) (as the $\pm$ part will be ± 0). When $\Delta = 1 \bmod 5$, we know that this parts gives us 2 solutions using the same reasoning as above.

For $\Delta = 1 \bmod 2$, we cannot directly use the discriminant to derive any information about the number of solutions, but there are only 4 quadratics in mod 2, so we can look up this one and find that it has 2 solutions $f(x) = x^2 + x = 0 \bmod 2$ (and this has 2 solutions in mod 2).

So there are 4 solutions in all $(2 \cdot 2 \cdot 1)$.

8)

8.a)

$$x^2 + bx + c = 0 \bmod 210 \tag{25}$$

$$210 = 5 \cdot 2 \cdot 3 \cdot 7 \tag{26}$$

To get 8 solutions, we need to have 3 of the prime factors have 2 solutions and the other one have 1 solution. Then we will have 8 solutions in all.

$$\begin{aligned}\Delta &= 1 \bmod 2 \\ \Delta &= 0 \bmod 3 \\ \Delta &= 1 \bmod 5 \\ \Delta &= 1 \bmod 7 \\ \Delta &= 141 \bmod 210\end{aligned} \tag{27}$$

$\Delta = 141 = b^2 - 4c \bmod 210$. $141 + 4c = b^2$ so b is odd. 169 is the next square after 141, so set $b^2 = 169, b = 13$. Then $141 + 4c = 169 \implies c = 7$.

Hence we get

$$x^2 + 13x + 7 = 0 \tag{28}$$

which has 8 solutions.

8.b)

$$\begin{aligned}f(x) &= 0 \bmod 143 \\ (x-a)(x-b)(x-c) &= 0 \bmod 143\end{aligned} \tag{29}$$

We want this to have 6 solutions mod 143.

We can split this into its prime factors, which is $143 = 11 \cdot 13$. We need to try and get 2 solutions mod 11 and 3 solutions mod 13 so that we have 6 solutions in all.

We know that $12 = 1 \bmod 11$, so we can exploit this fact to get a repeated root in mod 11 when there are distinct roots in mod 13.

$$\begin{aligned} f(x) &= (x-1)(x-5)(x-12) \\ &= (x-1)^2(x-5) \bmod 11 \\ &= (x-1)(x-5)(x-12) \bmod 13 \end{aligned} \tag{30}$$

As we can see, $f(x)$ has 2 solutions in mod 11 and 3 solutions mod 13. Hence $f(x)$ will have 6 solutions mod 143 by the CRT.